



Alignet

Políticas General del Sistema de Gestión de Seguridad de la Información

Responsable:	Oficialía de Seguridad y Cumplimiento
Fecha de Vigencia:	01 de setiembre de 2026
Código:	ALG-SEC-PG-01
Versión:	01

1. GENERALIDADES

1.1. Objetivos

- Crear un marco referencial para gestionar de manera apropiada la seguridad de la información de ALIGNET.
- Establecer las expectativas de la Alta Dirección con respecto al uso que los colaboradores deben hacer de los activos de información de ALIGNET, así como de las medidas que se deben adoptar para la protección de estos recursos.
- Concientizar a todos los colaboradores de ALIGNET sobre la importancia y la comprensión de sus responsabilidades individuales sobre seguridad de la información.
- Especificar las medidas de seguridad de la información que ALIGNET debe adoptar, para protegerse apropiadamente contra amenazas que podrían afectar la confidencialidad, integridad y disponibilidad de la información, las cuales podrían ocasionar alguna de las siguientes consecuencias:
 - Pérdida o mal uso de los activos de información.
 - Pérdida de imagen de ALIGNET frente a sus clientes y terceros.
 - Incumplimiento de las normas legales que debe cumplir ALIGNET.
 - Proporcionar a todos los colaboradores de ALIGNET los lineamientos que faciliten una adecuada toma de decisiones en aspectos relacionados a la seguridad de la información.

1.2. Base Legal y Normativa

- Payment Card Industry Data Security Standard (PCI DSS) v4.0.1
- Payment Card Industry 3-D Secure (PCI 3DS)
- Payment Card Industry Data Security Personal Identification Number (PCI PIN)
- Ley N° 29733 – Ley Protección de Datos Personales.
- Decreto Supremo N° 016-2024-JUS, que aprueba el Reglamento de la Ley de Protección de Datos Personales.
- ISO/IEC 27001:2022, Sistemas de Gestión de la Seguridad de la Información (SGSI)
- ISO/IEC 27002:2022, Código de prácticas para los controles de seguridad de la información
- Codificación de las Normas de la Superintendencia de Bancos de Ecuador.
- Ley N° 29440 - Ley de los Sistemas de Pagos y de Liquidación de Valores. Banco Central de Reserva del Perú (BCRP)
- Decreto Legislativo N° 1665: Modificación de la Ley de los Sistemas de Pagos y de Liquidación de Valores (BCRP)

- Circular N° 027-2022-BCRP: Reglamento de los Acuerdos de Pago con Tarjetas (APT)
- Ley N° 29985: Ley que regula las características básicas del dinero electrónico como instrumento de inclusión financiera.
- Resolución SBS N° 2116 2009: Reglamento de Gestión de Riesgos.
- Resolución SBS N° 789-2018: Norma para la prevención del lavado de activos y del financiamiento del terrorismo aplicable a los sujetos obligados bajo supervisión de la UIF-Perú.
- Resolución SBS N° 2351 2023: Modificación de la Norma para la prevención del lavado de activos y del financiamiento del terrorismo aplicable a los sujetos obligados bajo supervisión de la UIF-Perú.
- Resolución No. SB-2021-2126: Capítulo V - Norma de Control para la Gestión del Riesgo Operativo
- Resolución No. SB-2023-01901. Superintendencia de Bancos del Ecuador.
- Decreto Supremo N° 005-2023-MINCETUR: Reglamento de la Ley N° 31557 que regula los juegos a distancia y las apuestas deportivas a distancia.
- Mastercard Rules (MASTERCARD)
- Visa Core Rules and Visa Product and Service Rules (VISA)

1.3. Nivel de Aprobación

Este documento ha sido revisado y aprobado por la Alta Dirección de ALIGNET, incluyendo la Gerencia General y las jefaturas competentes en Perú y Ecuador, en conformidad con los requisitos regulatorios y de gobierno corporativo aplicables en ambas jurisdicciones. La Política General del Sistema de Gestión de Seguridad de la Información (SGSI) es de cumplimiento obligatorio para todas las operaciones, filiales y unidades de negocio de ALIGNET en Perú y Ecuador; ha sido validada por el Comité de Riesgos, Tecnología y Cumplimiento y su aprobación ha sido informada al Directorio y a la máxima autoridad gerencial en cada país.

1.4. Alcance

La presente Política General del Sistema de Gestión de Seguridad de la Información (SGSI) aplica a todas las actividades, procesos, personas, activos de información, tecnologías y terceros que tratan, almacenan o transmiten información de ALIGNET en las jurisdicciones de Perú y Ecuador.

1.5. Responsabilidades

1.5.1. Del Comité de Riesgos, Tecnología y Cumplimiento

- El Comité de Riesgos, Tecnología y Cumplimiento constituye la instancia colegiada de gobierno responsable de evaluar y supervisar, dentro de sus atribuciones, la gestión de Seguridad de la Información y Ciberseguridad de ALIGNET.
- En materia de Seguridad de la Información y Ciberseguridad, son funciones del Comité:
 - a) Revisar la evolución del Sistema de Gestión de Seguridad de la Información (SGSI), sus objetivos, riesgos y controles.
 - b) Revisar las políticas, procedimientos y metodologías de Seguridad de la Información y Ciberseguridad que correspondan.
 - c) Tomar conocimiento de los principales riesgos, vulnerabilidades, incidentes, indicadores y planes de tratamiento relacionados con Seguridad de la Información y Ciberseguridad.
 - d) Realizar seguimiento a las acciones de mejora y planes de remediación que correspondan.
 - e) Evaluar los resultados de auditorías, evaluaciones de seguridad y pruebas técnicas relevantes.
 - f) Elevar al Directorio aquellos asuntos que, por su criticidad, impacto, nivel de riesgo o requerimiento regulatorio, requieran su conocimiento o decisión.
- La conformación, periodicidad, atribuciones y demás reglas de funcionamiento del Comité de Riesgos, Tecnología y Cumplimiento se encuentran establecidas en su acta o documento de gobierno vigente.

1.5.2. De la Oficialía de Seguridad y Cumplimiento

- Asegurar que la Política General de Seguridad de la Información y los Objetivos del SGSI, se establezcan considerando los requisitos de la norma ISO/IEC 27001:2022 y sean compatibles con la planificación estratégica de ALIGNET.
- El Área de Seguridad de la Información es independiente de las funciones de negocio, TI, riesgos y auditoría, reporta a la máxima autoridad gerencial y lidera el establecimiento, implementación, mantenimiento y mejora continua del SGSI, definiendo estrategias y objetivos alineados a la estrategia institucional.
- Adicionalmente, asegurar la gestión integral de incidentes y el cumplimiento de las notificaciones regulatorias. Para ello, ALIGNET cuenta con mecanismos establecidos

para informar formalmente a la Superintendencia de Bancos sobre los incidentes que afecten a sus servicios críticos en un plazo máximo de cinco (5) días, garantizando la remisión del informe de causa raíz del problema en un plazo máximo de veinte (20) días.

1.5.3. De la Gerencia de Tecnología de la Información

- La Gerencia de Tecnología, trabaja en conjunto con la Oficialía de Seguridad y Cumplimiento, la aplicación de controles de Seguridad y Protección a los activos informáticos.

1.5.4. Del Departamento de Talento Humano

- Apoyar en la difusión de la Política General de Seguridad de la Información a todos los colaboradores de ALIGNET. Al plan de capacitación de seguridad de la información, incluirlo dentro del plan general.

1.5.5. De todos los colaboradores

- Cumplir la Política General del SGSI, los procedimientos, estándares y lineamientos vigentes, así como las obligaciones contractuales y regulatorias aplicables en Perú y Ecuador, participando en las capacitaciones y campañas de concientización programadas por la organización.
- Proteger la información y los activos bajo su custodia, respetando la clasificación de la información, utilizando únicamente herramientas autorizadas, y reportando de inmediato cualquier pérdida, acceso no autorizado, mal uso, o sospecha de incidente de seguridad a los canales definidos por el SGSI.
- Mantener la confidencialidad, integridad y disponibilidad de la información a la que acceden por razón de sus funciones, evitando la divulgación no autorizada, el almacenamiento en medios no aprobados y la transferencia por canales inseguros, de acuerdo con las políticas y controles definidos por la organización.
- Utilizar credenciales personales e intransferibles y activar los factores de autenticación requeridos; no compartir contraseñas ni dispositivos de autenticación, bloquear sesiones cuando no estén en uso y seguir las directrices de gestión de accesos e identidad establecidas por la organización.
- Tratar los datos personales conforme a las leyes aplicables y las directrices corporativas, respetando los principios de minimización, finalidad y confidencialidad, y utilizando exclusivamente los canales y herramientas autorizadas para su procesamiento y transmisión.

1.6. Glosario de Términos

- **Activo:** En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas, etc.) que tenga valor para la organización.
- **Análisis de Riesgos:** Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. El análisis de riesgos proporciona la base para la estimación de riesgos y las decisiones sobre el tratamiento de riesgos. El análisis de riesgos incluye la estimación de riesgos.
- **Banco de datos personales:** Es el conjunto de datos de personas naturales computarizado o no, y estructurado conforme a criterios específicos, que permita acceder sin esfuerzos desproporcionados a los datos personales, ya sea aquel centralizado, descentralizado o repartido de forma funcional o geográfica.
- **Datos personales:** Es aquella información numérica, alfabética, gráfica, fotográfica, acústica, sobre hábitos personales, de localización, identificadores en línea o de cualquier otro tipo concerniente a aspectos físicos, económicos, culturales o sociales de las personas naturales que las identifica o las hace identificables. Se considera identificable cuando se puede verificar la identidad de la persona de manera directa o indirectamente a partir de la combinación de datos a través de medios que puedan ser razonablemente utilizados.
- **Datos sensibles:** Es aquella información relativa a datos genéticos o biométricos de la persona natural, datos neuronales, datos morales o emocionales, hechos o circunstancias de su vida afectiva o familiar, los hábitos personales que corresponden a la esfera más íntima, la información relativa a la afiliación sindical, salud física o mental u otras análogas que afecten su intimidad.
- **Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales:** Es el órgano encargado de ejercer la Autoridad Nacional de Protección de Datos Personales a que se refiere el artículo 32 de la Ley, pudiendo usarse indistintamente cualquiera de dichas denominaciones en el presente Reglamento.
- **Directorio:** Persona o grupo de personas que dirige y controla una organización al más alto nivel. El Directorio (o alta gerencia) tiene el poder de delegar autoridad y proporcionar recursos dentro de la organización.
- **Propietario del Activo de Información:** funcionario responsable de la integridad, confidencialidad y disponibilidad de cierta información. Tiene autoridad para especificar, exigir las medidas de seguridad y otorgar niveles de accesos a los activos de información de su responsabilidad.

1.7. Gobierno del SGSI y Comités

El gobierno del Sistema de Gestión de Seguridad de la Información (SGSI) se articula mediante el Directorio, el Comité de Riesgos, Tecnología y Cumplimiento, la Oficialía de Seguridad y Cumplimiento y las áreas responsables de implementar y operar los controles de seguridad.

El Comité de Riesgos, Tecnología y Cumplimiento realiza la supervisión periódica de la Seguridad de la Información y Ciberseguridad, tomando conocimiento de los riesgos, indicadores, incidentes, vulnerabilidades, auditorías, evaluaciones de seguridad, planes de tratamiento y acciones de mejora relevantes.

La Oficialía de Seguridad y Cumplimiento coordina y supervisa la gestión del SGSI y de Ciberseguridad, manteniendo independencia respecto de las funciones responsables de implementar y operar los controles tecnológicos.

Las decisiones, acuerdos y acciones que se deriven de las sesiones del Comité deberán mantenerse documentadas conforme a los mecanismos de gobierno y gestión documental vigentes.

1.8. Unidad responsable del SGSI y de Ciberseguridad

La Oficialía de Seguridad y Cumplimiento es la unidad responsable de dirigir, coordinar, supervisar y reportar la gestión del Sistema de Gestión de Seguridad de la Información (SGSI) y de Ciberseguridad de ALIGNET, dentro de las funciones y atribuciones formalmente asignadas.

La función de Seguridad de la Información y Ciberseguridad opera con independencia de las áreas responsables de diseñar, implementar y operar los controles tecnológicos, con la finalidad de preservar la adecuada segregación de funciones.

Entre sus funciones se encuentran mantener el marco del SGSI, coordinar la identificación, evaluación y tratamiento de riesgos de Seguridad de la Información y Ciberseguridad, monitorear la eficacia de los controles, coordinar auditorías y pruebas técnicas, consolidar métricas e incidentes, verificar el cumplimiento normativo aplicable y reportar los asuntos relevantes al Comité de Riesgos, Tecnología y Cumplimiento y al Directorio, según corresponda.

La ejecución y operación técnica de los controles corresponde a las áreas tecnológicas, de monitoreo y demás funciones responsables definidas en las políticas y procedimientos específicos de ALIGNET.

2. POLÍTICA

2.1. Adhesión a la Política

- I. La presente política, los procedimientos y los estándares que tenga asociados, deben ser cumplidos por todos los colaboradores, proveedores de servicios y terceros sin excepción.
- II. La Oficialía de Seguridad y Cumplimiento debe monitorear el cumplimiento de las políticas, procedimientos y estándares del Sistema de Gestión de Seguridad de la Información a través de los procedimientos de revisión establecidos y el Oficial de Seguridad y Cumplimiento debe reportar los resultados al Directorio de ALIGNET.
- III. La presente Política debe ser revisada al menos una vez cada doce meses y actualizada según sea necesario para reflejar los cambios en los objetivos de ALIGNET o los posibles riesgos.
- IV. Las políticas, procesos, procedimientos y metodologías de seguridad se revisan al menos anualmente; son aceptados por el Comité de Riesgos, Tecnología y Cumplimiento y propuestos para aprobación del Directorio.

2.2. Marco de Ciberseguridad

- I. Con el objetivo de preservar la confidencialidad, integridad y disponibilidad de los activos de información, ALIGNET define y mantiene una estrategia y un marco de ciberseguridad alineado a las mejores prácticas internacionales. Este marco permite a la organización gestionar de manera resiliente y oportuna las amenazas, eventos e incidentes de ciberseguridad tanto internos como externos, y se estructura operativamente en las siguientes cinco funciones mínimas:
 - **Identificar:** Disponer y mantener procesos, prácticas, recursos humanos y tecnológicos orientados a identificar y evaluar los riesgos de ciberseguridad en los procesos de negocio. Esto incluye la búsqueda continua de debilidades o vulnerabilidades que podrían ser explotadas por actores de amenazas internos y/o externos.
 - **Proteger:** Diseñar, implementar y mantener medidas y controles preventivos de ciberseguridad de múltiples capas, con el fin de salvaguardar y defender los activos tecnológicos y la información crítica de ALIGNET.
 - **Detectar:** Diseñar, implementar y mantener actividades continuas para la detección e identificación oportuna de la ocurrencia de eventos de ciberseguridad. Esto contempla el registro continuo y centralizado de eventos, así como la gestión oportuna para facilitar alertas tempranas.
 - **Responder:** Desarrollar e implementar protocolos para tomar medidas inmediatas y oportunas ante la detección de un incidente de ciberseguridad, orientadas a contener su impacto dentro de la entidad. Para ello, ALIGNET

asegura la alineación e integración entre sus protocolos de ciberseguridad, gestión de crisis, planes de comunicación y planes de continuidad de negocio.

- **Recuperar:** Desarrollar e implementar actividades para mantener los planes de resiliencia operativa, garantizando la restauración de cualquier capacidad o servicio crítico que se haya visto afectado por un incidente de ciberseguridad, y logrando una recuperación oportuna hacia la operación normal.

2.3. Protección de la Información

- I. El Directorio y las Gerencias reconocen que la seguridad de la información es importante para ALIGNET y su protección debe ser impulsada y apoyada por todos los miembros de ALIGNET.
- II. La información es un activo valioso que debe ser protegido de manera consistente con los requerimientos legales, normativos y contractuales que sean aplicables en ALIGNET.
- III. Toda información generada por los colaboradores o proporcionada por ALIGNET para el desempeño de sus labores es de propiedad de ALIGNET, durante y luego de la finalización de la relación laboral, esto incluye información impresa o escrita en papel, almacenada electrónicamente, transmitida por correo o usando medios electrónicos.
- IV. Se debe tener presente que no es posible eliminar el riesgo, sólo mitigarlo, por lo tanto, los controles que se definan para proteger los activos de información deben ser determinados en base a un análisis de riesgo a los activos de información, el cual debe ser realizado periódicamente.

2.4. Apoyo del Directorio

- I. El Directorio de ALIGNET debe destinar los recursos necesarios para asegurar que todos los colaboradores reciban concientización permanente en seguridad de la información, de acuerdo a su función y rol.
- II. Para aquellos riesgos que no sean aceptables, deberán seleccionarse medidas de mitigación apropiadas, las cuales serán sometidas a la aprobación de la Gerencia General de ser el caso, para asegurar que:
 - Son suficientes para llevar el riesgo a un nivel apropiado.
 - Reciben los recursos y el apoyo necesarios para su implementación.

2.5. Análisis de Riesgos

- I. El Análisis de Riesgo comprende la identificación de los riesgos a los cuales están expuestos los activos de información de Gerencia de Tecnología, Unidad de Autenticación, Unidad de Adquirencia y Gerencia de Operaciones, mediante la identificación de las vulnerabilidades y las amenazas que las pueden explotar, la

probabilidad de ocurrencia y el impacto potencial sobre los procesos operativos de las Gerencias y Unidades de negocio.

- II. El análisis de riesgo de ALIGNET se realizará usando la Metodología de Gestión de Riesgos de Seguridad de la Información definida en el documento “ALG-SEC-MT-01 Metodología de Gestión de Riesgos de Seguridad de la Información”, el cual forma parte del Sistema de Gestión de Seguridad de la Información de ALIGNET.

2.6. Gestión de Riesgos

- I. La Gestión del Riesgo comprende establecer la estrategia a fin de eliminar, reducir, mitigar y/o transferir el riesgo estableciendo, según sea el caso, planes de mejora que comprenden políticas, procedimientos y controles en función al riesgo asociado y al activo(s) de información que ha sido evaluado.
- II. Estos planes de mejora deben tener un enfoque integrador de aspectos relacionados con el personal, los procesos y la tecnología, logrando reducir el riesgo e implementar las mejores prácticas, lo cual permite fortalecer el nivel de protección de la información. Dichos planes de mejora deben ser detallados por cada Gerencia y Unidad de Negocio, indicando responsabilidades y cronogramas para su implementación.

2.7. Clasificación de la Información

- I. Los Propietarios de Información y Custodios de Información clasifican la información que esté bajo su responsabilidad en “Restringida”, “Confidencial”, “Uso Interno” o “General o de Uso Público” de acuerdo con su importancia para el ALIGNET.

2.8. Uso de Activos de Información

- I. Todo uso de los activos de información debe ser para propósitos de las operaciones de ALIGNET de acuerdo con las políticas, estándares, procedimientos y manuales que definan.
- II. Se mantiene el ALG-SEC-FR-01 Inventario General de Activos dentro del alcance con clasificación por valor, requisitos legales, sensibilidad y criticidad, y con registro de propietario, custodio y ubicación. Los propietarios revisan y actualizan el inventario periódicamente.

2.9. Cumplimiento

- I. ALIGNET debe cumplir las disposiciones relacionadas a Seguridad de Información que emitan los Órganos Reguladores, así como sus Políticas Organizacionales.

- II. Se deben realizar auditorías de seguridad de la información al menos una vez al año por personal independiente y calificado, aplicando estándares vigentes; incluyen, como mínimo, pruebas de vulnerabilidad y penetración a infraestructura, redes, aplicaciones, bases de datos y canales.

2.10. Concientización

- III. El departamento de Talento Humano, a través del Plan de Capacitación se asegura que los colaboradores son conscientes de:
- IV. La importancia de la Política General de Seguridad de la Información y sus implicancias.
- V. Su contribución a la eficacia del Sistema de Gestión de Seguridad de la Información, incluidos los beneficios de su mejora.
- VI. Las consecuencias de no cumplir con los requisitos del Sistema de Gestión de Seguridad de la Información, se detallan en el Reglamento Interno de Trabajo.

2.11. Monitoreo y Revisión del Sistema de Gestión de Seguridad de la Información (SGSI)

- I. La efectividad de los controles del SGSI se monitorea, como mínimo, de forma semestral, dejando evidencia en informes con: KRIs y KPIs de control, avance de planes de tratamiento, mapas de riesgo (inherente/controles/residual), incidentes y hallazgos con su estado de remediación; el informe se presenta al Comité de Riesgos, Tecnología y Cumplimiento y sus acuerdos se elevan al Directorio.
- II. El desempeño del SGSI se evalúa anualmente considerando auditorías (incluye pruebas de vulnerabilidad y de penetración), incidentes, monitoreo continuo de controles, resultados de evaluación de riesgos y retroalimentación de partes interesadas; las acciones de mejora se aprueban por el Comité de Riesgos, Tecnología y Cumplimiento y se informan al Directorio para su aprobación y seguimiento.

2.12. Controles Técnicos de Seguridad de la Información

- I. Para asegurar la existencia de un apropiado ambiente de gestión de seguridad de la información, ALIGNET establece, implementa y controla los siguientes lineamientos técnicos obligatorios para la protección de sus activos:
 - Eliminación Segura de la Información: Se deben aplicar procedimientos para la eliminación de la información crítica de la entidad de manera segura, considerando en todo momento los requerimientos legales y

regulatorios aplicables. Este control se extiende a la eliminación de la información crítica en las bases de datos o repositorios de los proveedores de la entidad una vez concluida la prestación de sus servicios.

- **Gestión y Monitoreo de Usuarios Privilegiados:** Todo acceso privilegiado debe ser gestionado mediante la utilización de credenciales de usuarios personalizados y métodos de autenticación multifactor. Se debe garantizar el registro de la trazabilidad de las acciones ejecutadas y su monitoreo permanente. Las credenciales por defecto (default) en infraestructuras deben ser custodiadas por la Unidad de Seguridad de la Información y su uso será excepcional y debidamente autorizado.
- **Pistas de Auditoría (Logs):** Se deben mantener procedimientos que permitan contar con pistas de auditoría inalterables a nivel de dispositivos de infraestructura, aplicativos, bases de datos y sistemas operativos, que registren los cambios realizados a la información crítica. Queda estrictamente prohibido que los administradores tengan permisos para borrar o desactivar las pistas de sus propias actividades.
- **Criptografía y Llaves Criptográficas:** Se deben establecer procedimientos para regular el uso, la protección y el tiempo de vida de las llaves criptográficas utilizadas para cifrar la información de ALIGNET. Asimismo, se aplicarán técnicas de cifrado sobre la información que lo requiera como resultado del análisis de riesgos de seguridad.
- **Segmentación de Redes y Protección Perimetral:** Con base en el análisis de riesgos y la arquitectura tecnológica definida, se debe garantizar la segmentación de la red de datos de ALIGNET y la implementación de sistemas robustos de control y autenticación. Esto incluye, de manera enunciativa mas no limitativa, el uso de sistemas de prevención de intrusos (IPS), firewalls y firewalls de aplicaciones web (WAF), con el fin de minimizar los accesos no autorizados, especialmente a la información crítica.
- **Escaneo Automatizado de Vulnerabilidades:** Es obligatorio realizar el escaneo automatizado de vulnerabilidades en el código fuente para mitigar los riesgos de seguridad de las aplicaciones informáticas, tanto previo a su liberación (pase a producción) como de aquellas que ya se encuentran en el ambiente de producción.

- II. **Dominios mínimos de Seguridad de la Información y Ciberseguridad** - Los controles técnicos y operativos de Seguridad de la Información y Ciberseguridad de ALIGNET se desarrollan mediante los programas y procedimientos especializados del SGSI. Como mínimo, se consideran los siguientes dominios:

- Uso de medios de almacenamiento externo y removible: regulado mediante el ALG-SEC-PG-03 MPP del Programa de Aseguramiento de la Información y el ALG-SEC-PG-15 MPP del Programa de Conocimiento y Uso Aceptable.
- Uso de Internet, Intranet y Extranet: regulado mediante el ALG-SEC-PG-15 MPP del Programa de Conocimiento y Uso Aceptable y los controles de red establecidos en ALG-SEC-PG-12 MPP del Programa de Administración de Redes.
- Respalos de información: regulados mediante el ALG-SEC-PG-04 MPP del Programa de Gestión de Vulnerabilidades.
- Protección contra código malicioso: regulada mediante el ALG-SEC-PG-04 MPP del Programa de Gestión de Vulnerabilidades y el ALG-SEC-PG-15 MPP del Programa de Conocimiento y Uso Aceptable.
- Escritorio limpio y pantalla limpia: regulados mediante el ALG-SEC-PG-15 MPP del Programa de Conocimiento y Uso Aceptable.
- Seguridad de aplicaciones y desarrollo seguro: regulada mediante el ALG-SEC-PG-05 MPP del Programa de Aseguramiento del Ciclo de Vida de Desarrollo de Software.
- Seguridad perimetral y segmentación de redes: reguladas mediante el ALG-SEC-PG-12 MPP del Programa de Administración de Redes.
- Seguridad en servicios e infraestructura en la nube: regulada mediante el ALG-SEC-PG-12 MPP del Programa de Administración de Redes, complementada por los demás controles de Seguridad de la Información que resulten aplicables.
- Acceso remoto y teletrabajo: regulados mediante el ALG-SEC-PG-07 MPP del Programa de Gestión de Identidades y Accesos y el ALG-SEC-PG-12 MPP del Programa de Administración de Redes.
- Monitoreo de Ciberseguridad y gestión de incidentes de Seguridad de la Información: regulados mediante el ALG-SEC-PG-08 MPP del Programa de Monitoreo y Control de Ciberseguridad.
- La implementación de estos controles deberá considerar la criticidad de los activos, la evaluación de riesgos, el alcance aplicable y los requisitos legales, regulatorios, contractuales y de seguridad correspondientes.

2.13. Seguridad en Canales Electrónicos

- I. Con el objetivo de garantizar la seguridad en las transacciones y proteger la información y los recursos de los clientes frente a eventos fraudulentos o no autorizados a través de los diferentes canales electrónicos que expone o gestiona

la organización (tales como adquirencia transaccional, plataformas web, móviles u otros), ALIGNET adopta e implementa de manera obligatoria las siguientes medidas de seguridad:

- **Transmisión Segura y Enmascaramiento de la Información:** Toda transferencia de información confidencial o sensible de los clientes debe realizarse bajo estrictas condiciones de seguridad. Cuando dicha información se envíe mediante mensajería móvil, correo electrónico u otro mecanismo de notificación, esta deberá ser debidamente enmascarada. Asimismo, toda la información confidencial transmitida por canales de comunicación debe estar en todo momento protegida mediante el uso de técnicas de cifrado robustas y acordes con los estándares internacionales vigentes.
- **Protección Antimalware Permanente:** ALIGNET garantiza que todos sus canales electrónicos cuenten con software antimalware permanentemente actualizado.
- **Autenticación Fuerte y Claves Dinámicas:** Para la matriculación, registro de cuentas, ejecución de transacciones monetarias y acceso a canales electrónicos, ALIGNET exige la validación y verificación de la autenticidad del cliente a través de métodos de autenticación fuerte.
- **Monitoreo Inteligente y Prevención de Fraudes:** Se establecen procedimientos, mecanismos y sistemas digitales e inteligentes orientados al monitoreo constante de las transacciones y el comportamiento de los clientes en el uso de los canales electrónicos.